Version Number: 01-2019

U.S. Department of Commerce
U.S. Census Bureau

Privacy Impact Assessment
for
CEN29 Census Questionnaire Assistance (CQA)

Reviewed by: Byron Crenshaw, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.09.30 10:36:27 -04'00' 05/21/2020

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Census Bureau/Census Questionnaire Assistance System

Unique Project Identifier: 006-000402200 00-07-01-02-01-00

<u>Introduction</u>: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system

CEN29/CQA is a major application implemented for the 2020 Decennial Census effort and provides contact center support on behalf of the USCB.

Census Questionnaire Assistance (CQA) Program at the U.S. Census Bureau (USCB), managed by MAXIMUS Federal interfaces with respondents over the phone to assist them with responding to and completing census questionnaires or other Frequently Asked Questions (FAQs) about the 2020 Census. CQA facilitates responses by answering questions and, in some cases, by completing the interview with the respondent over the telephone.

(b) System location

The two CQA Cloud Service Provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) data centers are located in Highland Ranch, Colorado, and Sterling, Virginia with the CSP FedRAMP Security Operations Center and Network Operations Center located in Denver, Colorado. The CQA Program Management Office and the CQA Operational Command Center are located in Washington DC. During 2020 Census operations, CQA will utilize 10 contact centers located in Florida, Tennessee, Missouri, Arizona, Colorado, New York, Texas and South Carolina.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

The CEN29/CQA system interconnects with both the CEN05/Enterprise Censuses and Surveys Enabling (ECaSE) platform for outbound operations and the CEN18/Census Data Lake (CDL) platform for inbound and outbound operations reporting. This connectivity is managed via the Service Oriented Architecture (SOA) Enterprise Service Bus (ESB). In addition, CEN29/CQA interconnects with the CEN05/ECaSE Internet Self Response (ISR) system and CEN05/Nonresponse Follow-up (NRFU) systems to provide interfaces for the CQA Customer Service Representative (CSR) to access the Census questionnaire forms online, while authenticating the CSR against the CQA identity and access management system.

CEN29/CQA also interfaces with: the TTE Commercial datacenter to support Secure Development Life Cycle (SDLC) processes for code promotion purposes; the EPAY FedRAMP Cloud to provide access to timekeeping services to CQA operational staff, and; the Adobe Cloud to provide access to CQA operational staff access to training.

Additionally, CEN29/CQA interfaces with the following systems through Amazon Web Services based Application Programming Interfaces (API's) and file transfer utility:

- Oracle Talent Acquisition Cloud (OTAC) will be used to provision CQA accounts for these individuals to provide access to CQA applications and external cloud services such as EPAY/TKS and Adobe Connect.
- MAXIMUS Corporate SharePoint and CQA will both send and receive data necessary to CQA operations including daily briefings, standard operating procedures and knowledge articles.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

The CQA program is part of the overall 2020 Decennial Census effort and provides contact center support on behalf of the USCB. The CQA has two primary functions:

1. Provide assistance for respondents by answering questions about specific items on the 2020 Census questionnaire form or other FAQs about the Census.
    - **Tier 1:** Provide telephone assistance through an automated Interactive Voice Response (IVR) system.
    - **Tier 2:** Provide real-time assistance by a CSR over the telephone.
2. Provide an option for respondents to complete a 2020 Census interview over the telephone.

(e) How information in the system is retrieved by the user

After a Customer Service Representative (CSR) authenticates a valid user with the Census Bureau system, the specific inbound or outbound data collection instrument will display and allow the CSR to collect information from the respondent over the phone. For inbound operations, no respondent data is retrieved. A caller can provide an ID (sent to them via USPS mail) that will allow the CSR to retrieve an address associated with that ID. The CSR then verifies the address with the caller prior to full data collection for that household. If a caller does not have an ID, then the CSR will collect an address and the questionnaire responses from the caller.

For outbound operations, the Census Bureau provides the CQA contractor a list of case IDs and phone numbers for households that require some type of phone follow-up to confirm information. (These households had previously provided their census information.) Once a CSR is able to connect with someone over the phone during outbound operations, the case ID or phone number of record is required to proceed. After an eligible respondent is identified, the data collection instrument retrieves an address associated with that case ID which must be verified with the respondent. Previously supplied household roster information is then reviewed with the respondent.

(f) How information is transmitted to and from the system

A large outsourced contact center operation will support CQA program by executing inbound (respondent assistance) and outbound operations. The inbound operations will provide two main tiers of assistance:

- Tier 1 – The automated IVR system routes callers and provides answers to FAQs.

- Tier 2 – A CSR is the second tier of respondent support when IVR and web-based self-service tools have not been able to answer a respondent's question. The CSRs will have the ability to answer questions and capture respondent information into the ECaSE- Internet Self Response (ISR) system.

The outbound operation will provide support associated with maintaining and improving quality, specifically verifying respondent information for coverage improvement interviews.

- Encrypted Multi Protocol Label Switching (MPLS) is used to carry data and voice traffic between the call centers, network operation centers (NOC) /security operations centers (SOC)/Service Desk locations, and FedRAMP data centers
- Session Initiation Protocol (SIP) trunks to provide inbound/outbound call functions

Access to required Census-based applications will be facilitated from the FedRAMP data centers using firewalls, intrusion detection systems (IDS), URL filtering, traffic auditing, and logging functions All data traversing the FedRAMP boundary is encrypted and audited. This is implemented primarily through Secure Sockets Layer (SSL) for FedRAMP and web-based application services.

Data traversing to call centers, network security operation control centers, and for internal Census-based application or system interfaces will use IPsec/MPLS (Dynamic Multipoint Virtual Private Network [DMVPN]) to encrypt and secure traffic in transit. The delivery of recordings and transcription artifacts to the CEN18/CDL system is planned on a FIPS120-2 Level2 USB 3.0 compliant external storage media and will be delivered via approved courier provider FedEx to the USCB datacenter from CQA's Sterling VA datacenter location. The delivery of these recording artifacts (as zip archives) is scheduled to commence at the end of operations as part of close-out activities. This USB-based transfer of non-production based recordings to the external storage media shall also be conducted additional prior to operations for purposes of performance and resiliency testing. In both cases, the activation of the port to use for the USB-based transfer is approved per Risk Acceptance initiated by the CQA Government Program Management Office (GPMO) team.

(g) Any information sharing conducted by the system

Information sharing only occurs with USCB IT systems. CEN29/CQA system interconnects with both the CEN05/ECaSE platform for outbound operations and the CEN18/CDL platform for inbound and outbound reporting as detailed in the following paragraph. This connectivity is managed via the Service Oriented Architecture (SOA) Enterprise Service Bus (ESB). In addition, CEN29/CQA interconnects with the CEN05/ECaSE-ISR) system and CEN05/NRFU systems to provide interfaces for the CQA Customer Service Representative (CSR) to access the Census questionnaire forms online. This internet-based connectivity from CQA call center and OCC locations is managed per USCB enterprise guidance to leverage Akamai's Content Distribution Network (CDN) via the Amazon Trusted Internet Connection (ATIC).

The CEN29/CQA system shares data about activities and resources supporting CQA operations, including IVR and CSR interactions (average handle time [AHT], skill, disposition, and other survey data) with the CEN18/CDL system. Also, as part of Phase 2, the CEN29/CQA system will receive the workload to perform the outbound capability from CEN05/ECaSE for Coverage Improvement (CI) operations, and after CEN29/CQA performs the outbound operations, the closed cases' information will be sent back to CEN05/ECaSE as well as the CEN18/CDL systems.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The following authorities apply to CEN29 CQA:

13 U.S.C. 6(c), 141 and 193.

CEN29 CQA leverages USCB's Title 13 authority and obligations in conjunction with other federal statues and mandates for privacy, data security, transparency, and accountability, including the Privacy Act, the E-Government Act of 2002, FISMA and the Paperwork Reduction Act as well as federal standards and guidance promulgated by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The CEN29/CQA has an Authority to Operate (ATO) at Moderate Level from the Census Bureau.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
__X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): This PIA includes the addition of CEN29 outbound operations which was included in phase 1b and services from multiple FedRAMP Cloud Service Providers included in Phase 2.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015).

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID	X				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address		s. Physical Characteristics	
f. Race/Ethnicity	X	m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address		i. Business Associates	
b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History			
d. Work Telephone Number		h. Employment Performance Ratings or other Performance Information			
k. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice		f. Vascular Scan		i. Dental Profile	

Recording/Signatures					
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	
Telephone	X	Email			
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

A caller can provide an ID (sent to them via USPS mail) that will allow the CSR to retrieve an address associated with that ID. The CSR then verifies the address with the caller prior to full data collection for that household. If a caller does not have an ID, then the CSR will collect an address and the questionnaire responses from the caller. For outbound operations, the Census Bureau provides the CQA contractor a list of case IDs and phone numbers for households that require some type of phone follow-up. (These households had previously provided their census information.) Once a CSR is able to connect with someone over the phone during outbound operations, the case ID is required to proceed. After an eligible respondent is identified, the data collection instrument retrieves an address associated with that case ID which must be verified. Previously supplied household roster information is then reviewed with the respondent. These outbound operations calls are intended to improve the quality of a previously provided household roster and are part of overall Decennial operations to ensure the accuracy of the data.

CEN29 is a major application and uses a multitude of security controls mandated by the Federal Information Security Modernization Act of 2014 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include, but are not limited to data validation controls to ensure accuracy of information.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB Number 0607-1006
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID	X	Personal Identity Verification (PIV) Cards	
Other (specify):			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	X*	Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify): *This solution will enable the contact center to record interactions between respondents and CSRs across multiple sites and interactions, allowing the contact center to meet quality and regulatory compliance requirements. When the caller is connected to a CSR (for both inbound and outbound operations), the CQA system default is to start recording the interaction between the caller and the CSR. At the beginning of this interaction, the CSR will verbally inform the respondent that the call is being recorded for quality assurance purposes and ask the respondent for consent to continue recording the call. In the event the respondent declines consent, the CSR will stop the call recording immediately and continue with the call. These snippets of			

recordings from the beginning of the call up until the caller declines to be recorded will be deleted from CQA systems within 24 hours of the recording taking place.

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): For statistical purposes (To conduct the 2020 Census)			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The CQA program was established to aid in conducting the 2020 Decennial Census. The PII collected, maintained, and/or disseminated by the CEN 29 CQA consists of a 100% person count of the U.S. population including citizens, foreign nationals, or visitors. Data collection is used to generate national statistical information.

The CQA CSRs provide real-time assistance to the members of the public (respondents) over the telephone. The assistance function involves providing the type of information and support that will increase the public's participation in the Census, thereby improving the quality of the results and reducing costs. For the first time, telephone will serve as a primary response channel for the Decennial Census. The telephone channel will be promoted by the USCB as a data submission option.

This solution will enable the contact center to record interactions between respondents and CSRs across multiple sites and interactions, allowing the contact center to meet quality and regulatory compliance requirements. The recording solution provides reliable, high-quality recordings of both audio communications and desktop screen activity which will be provided to the Census Bureau as required.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Potential threats to privacy include:

- The collection of PII is required for the 2020 Census, therefore, a severe or substantial number of individuals would be affected if there was loss, theft or compromise of the data.
- CEN29 is also being managed by a third party and utilizing Cloud Service Provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) data centers.
- Although this IT system can only be accessed by authorized individuals that have a business need to know, the potential risk from insider threat to the organization, which may cause harm such as identity theft, embarrassment, loss of trust, or cost, still exists.

To process 2020 Decennial Census data maintained by the CQA system, security controls for the Federal Information Security Management Act (FISMA) moderate level must be implemented and validated through the FISMA Assessment and Authorization (A&A) process, using the USCB Risk Management Program System (RMPS) ATO method. This process includes implementing the NIST SP 800-53, 18 families of controls at the moderate level with additional controls and control steps from USCB policies as determined by the RMPS process. These controls include, but are not limited to, account management, authentication, physical controls, personnel security, security and privacy training, administrative controls, and technical controls such as Intrusion Detection/Prevention

System (IDS/IPS), Firewalls, use of Amazon Trusted Internet Connection (ATIC), and encryption of databases (Data at rest).

The Contact Recording System is delivered using a system called Calabrio. This solution will enable the contact center to record interactions between respondents and CSRs across multiple sites and interactions, allowing the contact center to meet quality and regulatory compliance requirements. The recording solution provides reliable, high-quality recordings of both audio communications and desktop screen activity which will be provided to the Census Bureau as required. The Contact Recording Solution implements security controls such as encryption, usage restriction, authentication, monitoring and logging. In addition, the CQA Contact Centers have policies and measures in place such as a paperless environments and prohibiting the use of non-government cell phones and other electronic devices in the call center area. This effectively prohibits CSRs from recording respondent information outside of the CQA solution.

The delivery of recordings and transcription artifacts to the CEN18/CDL system is planned as a SOA-based interface that will be delivered via the Managed File Transfer (MFTv2) service provided by USCB. This service is the same one used to transmit Agent paradata throughout 2020 Operations. Encrypted MPLS is used to carry data and voice traffic between the call centers, NOC/SOC/Service Desk locations, and FedRAMP data centers

- SIP trunks to provide inbound/outbound call functions

Access to required Census-based applications will be facilitated from the CSP FedRAMP data centers using firewalls, IDS, URL filtering, traffic auditing, and logging functions.

The delivery of recordings and transcription artifacts to the CEN18/CDL system is planned on a FIPS120-2 Level2 USB 3.0 compliant external storage media and will be delivered via approved courier provider FedEx to the USCB datacenter. The delivery of these recording artifacts (as zip archives) is scheduled to commence at the end of operations as part of close-out activities. This USB-based transfer of non-production based recordings to the external storage media shall also be conducted additional prior to operations for purposes of performance and resiliency testing.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau		X	X
DOC bureaus			
Federal agencies			
State, local, tribal gov’t agencies			
Public			
Private sector			

Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: The CEN29/CQA interfaces with the CEN18/ CDL to provide data about activities and resources supporting Census Questionnaire Assistance operations, including IVR and CSR interactions (average handle time [AHT], skill, disposition, and other survey data). Also, as part of Phase 2 (of the CQA contract), CEN29/CQA will receive the workload to perform the outbound capability from CEN05/ECaSE-OCS, and after CQA performs the outbound operations, the closed cases' information will be sent back to CEN05/ECaSE-OCS. The CEN29/CQA interfaces with CEN05/ECaSE-ISR, CEN05/NRFU-ISR and CEN05/NRFU-ENUM tools to pass specific parameters, such as case ID and CQA call ID, to provide interfaces for CSRs in the CQA Operation to input respondent Census Questionnaire data. The delivery of recordings and transcription artifacts to the CEN18/CDL system is planned as a SOA-based interface that will be delivered via the Managed File Transfer (MFTv2) service provided by USCB. This service is the same one used to transmit Agent paradata throughout 2020 Operations. The delivery of the recording artifacts (as zipped encrypted archives on an external storage device) is scheduled to commence at the end of operations as part of close-out activities. CEN29/CQA interfaces with the TTEC Commercial datacenter to support SDLC processes for code promotion purposes. CEN29/CQA interfaces with EPAY FedRAMP Cloud to provide access to timekeeping services to CQA operational staff. CEN29/CQA interfaces with Adobe Cloud to provide access to CQA operational staff access to training. CEN29/CQA interfaces with the following systems through Amazon Web Services: • Oracle Talent Acquisition Cloud (OTAC) will be used to provision CQA accounts for these individuals to provide access to CQA applications and external cloud services such as EPAY/TKS and Adobe Connect. • Microsoft Government Community Cloud (GCC) will host the MAXIMUS corporate SharePoint. CQA will both send and receive data necessary to CQA operations including daily briefings, SOPs, knowledge articles. CEN29/CQA uses a multitude of security controls mandated by the FISMA and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) Special Publication 800 series. These security controls include, but are not limited to the use of mandatory access controls, intrusion detection systems, intrusion prevention systems,

	anti-virus solutions, enterprise auditing/monitoring and encryption. Encryption of data at rest and in transit is implemented by encrypting the databases, applying FIPS 140-2 encryption at the border firewalls and implementing SAN-level encryption.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.census.gov/about/policies/privacy/privacy-policy.html	
X	Yes, notice is provided by other means.	Specify how: Specify how: During all inbound calls to CQA, there is a prerecorded message notifying callers being transferred to a CSR that their call will be recorded for Quality Assurance purposes. When the caller is connected to a CSR (for both inbound and outbound operations), the CQA system default is to start recording the interaction between the caller and the CSR. At the beginning of this interaction, the CSR will verbally inform the respondent that the call is being recorded for quality assurance purposes and ask the respondent for consent to continue recording the call. In the event the respondent declines consent, the CSR will stop the call recording immediately and continue with the call. These snippets of recordings from the beginning of the call up until the caller declines to be recorded will be deleted from CQA systems within 24 hours of the recording taking place.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an	Specify why not: You cannot opt out of participation in a

	opportunity to decline to provide PII/BII.	Decennial Census. The respondents do have an option to respond online, via paper or provide input to a Census field worker who shows up at their household rather than providing input through CQA.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: You cannot opt out of participation in a Decennial Census.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: In the event that the Census Bureau receives a Privacy Act request from a respondent, a text transcript of that recording could be provided.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Only authorized personnel are allowed to access PII within a system. Access to Information Systems and data that handle PII, as well as significant system events, are logged. All manual extractions for PII are logged, reviewed and recorded per Department of Commerce Policy, USCB, NIST SP 800-53 Appendix J Privacy Control Catalog, and specifically NIST SP 800-53 control AU-03, Content of Audit records. Procedures are in place for reporting and handling of inappropriate or unusual activity.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): December 13, 2019 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.

X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The CQA program employs a multitude of layered security controls to protect PII at rest, during processing, as well as in transit. The CQA program also follow the National Institute of Standards and Technology (NIST) standards including Special Publications (SP), NIST SP 800-63, NIST SP 800-37 and NIST 800-53 security controls. At a minimum, the following enterprise-level security controls are deployed and managed including, but not limited to the following:

- Intrusion Detection Systems (IDS) | Intrusion Prevention Systems (IPS)
- Firewalls and FIPS 140-2 encryption applied at the Border Firewalls
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest),
- All stored recordings for Calabrio have both application layer encryption, as well as AES 256-bit drive level encryption.
- All data stored within CQA is encrypted on self-encrypting drives.
- RSA Token with 2-Factor Authentication
- Access Controls
- Data Loss Prevention (DLP) solution
- All components are located in a secure location and only authorized personnel have access to components.

All data traversing the FedRAMP boundary is encrypted and audited. This is implemented primarily through Secure Sockets Layer (SSL) for FedRAMP and web-based application services.

Data traversing to call centers, network security operation control centers, and for internal Census-based application or system interfaces will use IPsec/MPLS (Dynamic Multipoint Virtual Private Network [DMVPN]) to encrypt and secure traffic in transit.

Any system within the CQA that contains, transmits, or processes PII has a current authority to operate (ATO) and goes through continuous monitoring process to ensure controls are implemented and operating as intended. The CQA continuous monitoring program will conduct security

certifications, vulnerability assessments, annual security control assessments (SCA), and testing and evaluation of the CQA program as part of the ongoing system development and life cycle process.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

_X_ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/CENSUS-5, Decennial Census Program- http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-5.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: GRS 3.1 GRS 3.2 GRS 4.3 N N1-029-10-5 Item M
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:

X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X
Other (specify):			

<u>Section 11</u>: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Combined data elements (Telephone number, name, and voice recordings and screen captures of respondent Census data) uniquely and directly identify individuals.
X	Quantity of PII	Provide explanation: A serious or substantial number of individuals affected by loss, theft, or compromise. Serious collective harm to individuals, harm to the organization’s reputation, or cost to the organization in addressing a breach.
X	Data Field Sensitivity	Provide explanation: Data fields, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.
X	Context of Use	Provide explanation: Disclosure of the PII itself may result in serious harm to the individual or organization.

X	Obligation to Protect Confidentiality	Provide explanation: 13 U.S.C. § 9 requires that data collected by the Census Bureau in its surveys, including the Decennial Censuses, shall remain confidential.
X	Access to and Location of PII	Provide explanation: System has access, physical and environmental controls that have been assessed by OIS. Located on computers and other devices on a network controlled by the organization. Access limited to a multiple populations of the organization's workforce beyond the direct program or office that owns the information on behalf of the organization- owned equipment outside of the physical locations owned by the organization only with a secured connection (e.g., virtual private network (VPN)). Backups are stored at CSP FedRAMP contractor-owned facilities and protected according to NIST/FedRAMP requirements.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The collection of PII is required for the 2020 Census, therefore, a severe or substantial number of individuals would be affected if there was loss, theft or compromise of the data.

CEN29 is also being managed by a third party and utilizing Cloud Service Provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) data centers.

Although this IT system can only be accessed by authorized individuals that have a business need to know, the potential risk from insider threat to the organization, which may cause harm such as identity theft, embarrassment, loss of trust, or cost, still exists.

Confidentiality is the key element that the Census Bureau reviews as part of the system categorization. Confidentiality, Integrity and Accessibility are the cornerstones of our IT/Cybersecurity program. We ensure that those security controls relating to the confidentiality of our data are fully assessed and operating as intended during the assessment process and through our continuous monitoring program. Controlled access to this IT system is based on the requirements set forth by the FISMA of 2014 and validated through the Assessment and Authorization (A&A) process as mandated by FISMA, using the USCB Risk Management Program System (RMPS) ATO method. This process utilizing the USCB Risk Management Framework (RMF) methodology includes

implementing NIST SP 800-53 controls at the "moderate" level with additional controls and control steps from USCB policies as determined by the RMPS process. These controls include, but are not limited to, account management, authentication, physical controls, personnel security, security and privacy training, and administrative controls. The Census Bureau conducts routine security awareness training on recognizing and reporting potential indicators of insider threat

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.